# EXHIBIT 1

ORIGINAL



# UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
A single story residence located at 3052 West Cheryllyn Lane in Anaheim, California, as described in Attachment A

Case No. 2:18-MJ-00484

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B



The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. §§ 2252A(a)(2); 2252A(a)(5)(B) | See attached Affidavit |

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Bernell E. Trapp, Task Force Officer
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 03-05-18

*Judge's signature*

City and state: Los Angeles, California

R.A. Oliver, USMJ
*Printed name and title*

SAUSA: Stacey R. Fernandez, x3152

**ATTACHMENT A**

PREMISES TO BE SEARCHED

The premises to be searched is a single story residence located at 3052 West Cheryllyn Lane in Anaheim, California (the "SUBJECT PREMISES"). The SUBJECT PREMISES is a single story, single-family condominium unit located on the west side of Beach Boulevard between Orange Avenue and Ball Road. The condominium complex is white with blue trim. The condominium is a single-family unit within a multi-unit complex. The SUBJECT PREMISES is on the second level of the complex, and the front door faces west. The numbers "3052" are attached above the entrance door of the residence. The SUBJECT PREMISES contains a garage which is located on the bottom level of the complex, with the living quarters located above.

**ATTACHMENT B**

ITEMS TO BE SEIZED

The items to be seized are evidence, contraband fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (distribution and attempted distribution of child pornography) and 2252A(a)(5)(B) (access with intent to view and possession of child pornography), specifically:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256.

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Any and all records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to peer-to-peer file sharing software.

g. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.

h. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of the SUBJECT PREMISES.

i. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession and/or use of any digital device(s) found inside the SUBJECT PREMISES.

j. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

a. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related

communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

**I. SEARCH PROCEDURE FOR DIGITAL DEVICES**

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of

the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be

seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, with respect to any person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant, the law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of the person onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of the person with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

RM

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

x

**AFFIDAVIT**

I, Bernell E. Trapp, being duly sworn, declare and state as follows:

## I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search the premises located at 3052 W. Cheryllyn Lane, Anaheim, California 92804 (the "SUBJECT PREMISES"), more fully described below and in Attachment A, which is attached hereto and incorporated herein by reference, and to seize evidence, fruits, and instrumentalities, as specified in Attachment B, which is also attached hereto and incorporated by reference, of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography).

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

## II. BACKGROUND FOR TFO TRAPP

3. I am a Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI") and have been so employed for more than twelve years. During my tenure as a Task Force

Officer, I have conducted and participated in numerous investigations of criminal activity. During these investigations, I have executed and participated in the execution of numerous search and arrest warrants and seized evidence of violations of federal law. I have conducted numerous investigations of child exploitation and child pornography. I have attended training classes concerning computer crimes, child pornography, and sexual exploitation of children, including trainings hosted by the Internet Crimes Against Children ("ICAC"). I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

4. Through my training and experience, and the training and experience of other law enforcement officers experienced in investigating crimes involving the sexual exploitation of children, with whom I have had discussions, I have become familiar with the methods used by people who commit these types of offenses. My training and experience has given me an understanding of how people who commit offenses relating to the sexual exploitation of children use the Internet to facilitate and commit those offenses.

## III. PREMISES TO BE SEARCHED

5. The premises to be searched is a single story residence located at 3052 West Cheryllyn Lane in Anaheim, California (the "SUBJECT PREMISES"). The SUBJECT PREMISES is a single story, single-family condominium unit located on the west side of Beach Boulevard between Orange Avenue and Ball Road. The

condominium complex is white with blue trim. The condominium is a single-family unit within a multi-unit complex. The SUBJECT PREMISES is on the second level of the complex, and the front door faces west. The numbers "3052" are attached above the entrance door of the residence. The SUBJECT PREMISES contains a garage which is located on the bottom level of the complex, with the living quarters located above.

## IV. SUMMARY OF PROBABLE CAUSE

6. On August 12, 2017, an individual using the mobile messaging application "Kik" sent me a link to a Dropbox account containing approximately 42 files of suspected child pornography. On the same date the user told me that he had previously had sex with a five year old and a seven year old. The IP address from which the link was sent is subscribed to the SUBJECT PREMISES.

## V. BACKGROUND REGARDING CHILD EXPLOITATION OFFENSES, COMPUTERS, AND THE INTERNET

7. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in Title 18, United States Code, Section 2256. The term "computer" is defined as set forth in Title 18, United States Code, Section 1030(e)(1). "Child erotica" means materials or items that are sexually arousing to persons who have a sexual interest in minors, but that are not, in and of themselves, legally obscene, or do not necessarily depict minors in sexually explicit conduct.

8. Based upon my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers and child pornography:

a. Internet. The term "Internet" is defined as the worldwide network of computers – a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider, which operates a host computer with direct access to the Internet.

b. Internet Service Providers. Individuals and businesses obtain access to the Internet through internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often

include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

c. Internet Protocol Addresses. An Internet Protocol ("IP") Address refers to a unique numeric or alphanumeric address used to connect to the Internet. IP Addresses can be "dynamic," meaning that the ISP assigns a different unique number to a device every time it accesses the Internet, or "static," meaning an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. There are two versions of IP addresses: IPv4 and IPv6. IPv4 is the most widely used IP, and uses four groups of numbers separated by periods in a 32-bit address scheme (e.g., 121.56.97.178). IPv6 uses colons to separate eight alphanumeric groups (e.g., 2001:0:1760:e3e7:1858:2cea:d075:6c4c). In a simple example, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is more typical is that one home may connect multiple digital devices to the internet simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home connect to the Internet via a router or hub. The devices connect to the router or hub, and the hub connects to the Internet. Internet activity from every device attached to

the router or hub is using the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. Most ISPs maintain records of which subscriber was assigned to which IP Address during an online session.

d. Kik Messenger. Kik Messenger, commonly called "Kik," is an instant messaging mobile application that allows users to transmit and receive messages, photos, videos, sketches, webpages, and other content after users register a username. Kik is known for preserving users' anonymity and allows users to register without providing a telephone number, however, the application records users' IP addresses.

e. Dropbox. Dropbox is a provider of electronic communication and remote computing services, including remote or "cloud" storage. Dropbox creates a folder on the user's computer, the contents of which are then synchronized to Dropbox's servers and to other computers and devices on which the user has installed Dropbox, keeping the same files up-to-date on all devices. Dropbox Basic users are given two gigabytes of free storage space. Dropbox Plus users are given one terabyte of storage space, as well as additional features, including advanced sharing controls, remote wipe, and an optional Extended Version History add-on.

## VI. Training and Experience in Computer-Related Sexual Exploitation Investigations

9. Based on my training and experience, and the training and experience of other law enforcement officers experienced in

investigating crimes involving the sexual exploitation of children with whom I have had discussions, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Individuals with an interest in child pornography can easily use a scanner to transfer printed photographs into a computer-readable format. Furthermore, with the advent of digital cameras, when a photograph is taken, it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera can be stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive on the camera. The video files can then be easily transferred from the camcorder to a computer. Digital cameras built into smartphones make the photos even easier to transfer to other devices.

c. Modems allow any computer to connect to another computer through the use of telephone, cable, or wireless

connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the methods of distributing and receiving child pornography. Child pornography can be transferred via electronic means to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., Instant Messaging), and easy access to the Internet, the computer is a preferred method for distributing and receiving child pornography.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera or smartphone, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them).

e. Media storage devices can easily be concealed and carried on an individual's person. It is particularly common for individuals to regularly carry their smart phones on them. These devices can store thousands of images of child pornography and connect directly to the Internet as well as other cellular devices.

f. The Internet affords individuals many different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

g. Individuals can also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL, Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

h. As is the case with most digital technology, communications via a computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many

places (temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

## VII. STATEMENT OF PROBABLE CAUSE

10. The following is based on information I learned from my conversations with FBI agents and other law enforcement officials, my own participation in the investigation, and my training and experience.

11. On August 12, 2017, I posted an advertisement on Craigslist seeking to connect with individuals interested in "taboo," a term used to refer to various sexual acts, including sex with children. An individual responded to the advertisement and I asked the individual if they could continue the conversation on Kik. I continued to communicate with the individual via Kik, where the individual's profile name is "talleyho14" ("TALLEYHO"). My Kik profile displayed only my undercover Kik username and profile name and no other personal information. That communication included the following:

a. TALLEYHO told me that he is a 30 year-old named Jake who lives in Orange County and that he is married so "discretion is a must."

b. TALLEYHO sent me a link to a Dropbox account with the message, "check this out." I opened the link and found that the account contained approximately 42 video files.

c. TALLEYHO told me that s/he had previously had sex with a five year old and a seven year old, saying "I came inside the 5 yo," and "Then a week later I came inside the 7yo." Between August 12, 2017, and August 15, 2017, TALLEYHO also talked about having sex with the OCE's nine year old daughter.

12. I reviewed thumbnail photographs of the video files contained in the Dropbox account that TALLEYHO sent and formed the opinion that the majority depicted child pornography. The thumbnail photographs include the following:

a. What appears to be a toddler female, approximately 3-5 years old, standing between the legs of a nude, adult male. The male has an erect penis, and it appears as if the toddler's elbow is rubbing against the male's penis.

b. What appears to be a nude female, approximately 2-5 years old, laying on her back on a bed. The female's legs are spread, exposing her vagina.

c. What appears to be a nude, prepubescent female laying on her back. The female's legs are spread and raised into the air. An adult male is rubbing his erect penis against the female's anus.

13. On August 13, 2017, Kik responded to a request for information associated with username "talleyho14." (the "Subject Account"). According to Kik, between June 29, 2017, and August 1, 2017, the Subject Account used IP address 172.90.36.99 (the "Suspect IP Address") on 19 different occasions, including on August 12, 2017, to log into "KIK" Account "talleyho14."

14. On August 14, 2017, ISP Charter Communications responded to a request for information associated with the Suspect IP Address. According to Charter Communications, the Subscriber Account using IP Address 172.90.36.99 on August 12, 2017, was assigned to "Maca Ortiz" at the SUBJECT PREMISES. Based on this information, I believe that when TALLEYHO shared the suspected child pornography with me on August 12, 2017, s/he did so from the SUBJECT PREMISES.

15. On or about February 13, 2018, I conducted surveillance at the SUBJECT PREMISES and found that all the Wi-Fi networks in range of the SUBJECT PREMISES were password protected. As such, only people with access to the password could access the networks.

16. On or about February 13, 2018, I directed Special Agent Amy Whitman to search a law enforcement database; SA Whitman determined that the name "Maca Ortiz" continues to be associated with the SUBJECT PREMISES.

## VIII. TRAINING AND EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

17. Based the facts set forth above, and my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, there is probable cause to believe that TALLEYHO has a sexual interest in children and images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement

officers with whom I have had discussions, there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in-person, in photographs, or in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children sometimes possess hard copies of child pornography, such as pictures, films, video tapes, magazines, negatives, photographs, etcetera. As digital technology has developed, individuals with a sexual interest in children or images of children have become much more likely to maintain child pornography in digital or electronic format,

stored either on digital devices, as defined in ¶ 18, or in remote storage locations on the Internet. Regardless of whether these individuals collect their child pornography in hard copy or digital format, they may maintain their child pornography for a long period of time, even years. They usually maintain these collections in a safe, secure, and private environment, such as their homes, vehicles, or nearby, so they can view the child pornography at their leisure. These collections are typically highly valued.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; may conceal such correspondence as they do their sexually explicit material; and may often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children typically prefer not to be without child pornography for prolonged periods of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f. Based on my training and experience, as well as my conversations with digital forensics agents, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via computer. Electronic files downloaded to

a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Because computer evidence is recoverable after long periods of time, and because there is probable cause to believe that persons at the SUBJECT PREMISES were once in possession of child pornography and likely obtained it from some as yet unidentified source, there is probable cause to believe that evidence of activity related to

the possession and distribution of child pornography, will be found at the SUBJECT PREMISES.

## IX. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

18. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital

devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could

contain as many as approximately 450 full run movies or 450,000 songs.

d. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were

created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

e. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

f. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as

a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

19. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. As previously discussed, the target of the investigation used Kik. I know that Kik is primarily, if not exclusively, used in mobile devices. In addition, Kik provided information that showed that the Subject Account was accessed via T-Mobile. Based on my experience and training, I know that T-Mobile is a popular cellular service provider.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock

their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these

companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that

are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

20. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

21. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

22. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of

the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual who is found at the SUBJECT PREMISES and reasonably believed by law enforcement to be a user of the device to unlock the device using biometric features in the same manner as discussed in the following paragraph.

23. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the SUBJECT PREMISES and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or fingerprints on

the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

24. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

## X. CONCLUSION

25. For all the reasons described above, there is probable cause to believe that evidence, fruits, and instrumentalities of

violations of the Subject Offenses, as described in Attachment B of this affidavit, will be found in a search of the SUBJECT PREMISES, as further described above and in Attachment A of this affidavit.

Bernell E. Trapp, Task Force Officer
Federal Bureau of Investigation

Subscribed to and sworn before me
this 5th day of March, 2018.

HONORABLE R. A. OLIVER
UNITED STATES MAGISTRATE JUDGE